Barclay Damon Live Presents *Cyber Sip*™ Episode 30: "Big Changes Coming to NYS's Part 500 Cybersecurity Rule"

Speakers: **Kevin Szczepanski**, Barclay Damon

[Kevin Szczepanski]: Hey, everyone, this is a *Barclay Damon Live* broadcast of the *Cyber Sip*. Practical talk about cybersecurity. I'm your host, Kevin Szczepanski. Let's talk.

[Kevin]: Hey, everyone. It's been six years since the New York Department of Financial Services enacted the first Part 500 cybersecurity rules for financial companies. So we were overdue for change. But change is here—or nearly here. Last July, the department issued the first of two proposed amendments to the rule, and in November it issued the second round of amendments. The 60-day comment period for the second round expired last month. So if we're asked here, we would tell you that we're probably due for a new cybersecurity rule sometime in the next 30 to 90 days. What will that rule mean for your business? Well, it depends on what kind of business you are. The rule applies chiefly to covered entities. What's a "covered entity"? It is an entity that is licensed, regulated, chartered, or otherwise authorized to do business under the New York banking law, insurance law, or financial services law. But even if you're not a covered entity, if you're a vendor to one, or you perform services for one, you should probably pay attention as well. Because if the covered entity has to change its cybersecurity rules internally, it's probably going to ask you to change yours as well. So what are the changes coming to New York's cybersecurity rules? We've broken them down into five categories and we're going to run down each one of them right now.

[Kevin]: Category one is risk assessments. And while this is a category and requirement under the current cybersecurity rules, the proposed new rules will deepen this requirement in a couple of ways. First, a risk assessment must be narrowly tailored to the covered entity's specific circumstances. What does that mean? Well, it means that you're going to have to take into account the covered entity's age, governance, services, products, operations, customers, vendors, and more. There's actually a non-exclusive list of 13 factors in the current proposed rule, and this risk assessment must be revisited and updated at least annually, or when a change in the company causes a change in its overall cyber risk posture.

[Kevin]: The second category, security controls. And I want to highlight three of them for you. One, MFA, two, passwords, and three, limited user access privileges. Now, in the current rule, MFA—or its equivalent—is required as a general matter. But in the proposed new rule, MFA, or multi-factor authentication, will be required for remote access and privileged accounts, or any accounts that are able to add, change, or remove users, or make operational changes to your system. Next passwords. Now you're probably one of the overwhelming majority of covered entities that still use passwords as an authentication device. And under the new rule, you will still be able to do so. But what you will need to do is develop a written password policy that meets industry standards. Now, the DFS does not tell us what "industry standards" are. It's not a defined term, but you can do no worse than consult NIST. The National Institute of Standards and Technology, and NIST has published Special Publication 800-63B. Now this is a tome as password discussion goes. It's a document over 70 pages long with just a few pages devoted to passwords, and it's really worth a read if you'd like to know more. Spoiler alert: The most important security control for passwords is length. Finally, limited user access privileges. Basically, you just want to make sure that the only people who have access to certain data and systems are the people that actually need it to perform their work. No one else should have that access.

[Kevin]: Category three, testing and training. Now, you already have an incident response plan. The proposed new rules will require you to have a business continuity and disaster recovery plan as well. The IRP makes sure that you are ready to respond and recover as quickly as possible from a data breach. And the business continuity and disaster recovery plan will make sure that you can restore normal business operations as quickly and efficiently as possible. More important, you will have to test these plans at least annually. That's a critical development, because testing these plans will make sure that you and your team have the muscle memory that they need to execute these plans when there is a cyber incident. You don't want to be dusting off your incident response plan, your business continuity and disaster recovery plan, for the first time, when you suffer a data breach. You want to be ready to go when this inevitably happens. And this annual testing requirement will help you get there.

[Kevin]: Next, under testing and training, you must develop policies and procedures for vulnerability management. Two ways you'll be required to do this: Vulnerability scanning and penetration testing. Now vul scanning is an automated means of testing your information system to identify weaknesses that a cybercriminal could exploit. Identifying them enables you to report them to your information security professionals and remediate them so they're no longer a problem. Penetration testing is a deeper kind of vulnerability management. That's where you hire an ethical hacker to come in and try to break into your system from the inside and the outside. There's no better way of identifying the weaknesses in your system and remediating them before a real cybercriminal comes into play.

[Kevin]: The third item under testing and training is one of the most important. Going forward on at least an annual basis, you'll have to conduct awareness training for all personnel in your organization, including social engineering exercises. That's so critically important. Why? Because, let's face it, our employees are on the front line of our information security. So teaching our employees how to recognize email, voicemail, and text-based phishing attacks is one of the best ways that you can secure your data and your networks from intruders.

[Kevin]: Second item under new governance requirements, your CISO will now be required to report to the board in three new areas. First, any plans for remediating "material inadequacies," and that is again a term that is not defined. Second, your CSO must report to the board any major cyber events. And third, your CISO must provide updates to your covered entity's risk assessment. The third item under new governance requirement is perhaps the most critical, and that is that the board or governing body of the covered entity must provide oversight and direction on cyber risk management. And in order to do that, the new proposed rule will require boards of directors to have sufficient knowledge and experience on their own, or to be advised by outside experts who do have sufficient knowledge and experience to effectively oversee cyber risk management. I think next to training, this is the most important development in the new proposed rules.

[Kevin]: What's going on here? The DFC is saying that the days of cybersecurity resting in the IT department or in the CISOs hands are over. Ultimately, the security of your data and your systems rests in the arms of the board or your governing body. The board must oversee your cybersecurity management, and the board must provide direction with respect to cybersecurity. And in order to do that, the board has to have the expertise to provide that guidance. So going forward—and I think some boards have already adopted this—you're going to want to have at least one person on your board with a cybersecurity background. You may want to have a standing cybersecurity or information security committee. And if you can't do either of those in the short term, you'll want to retain experts, forensic information security experts, that can provide strategic advice to the board of directors on how best to manage cybersecurity issues. Oh, and one last item I want to tell you about under new governance requirements.

[Kevin]: Under the current rules, a covered entity must annually certify its compliance, and the certification must be signed by a senior officer. Going forward, under the proposed new rules, however, the certification must be signed by both the CSO and the CEO. So the chief officer of the company must attest to its compliance. There's also an option under the proposed new rules to acknowledge less than full compliance with the

cybersecurity rules. But in order to do that, you have to identify deficiencies, state a plan, and your intention for remediating them and a timetable for doing so.

[Kevin]: Category five: notice requirements. Now, under the current cybersecurity rules, a covered entity must notify the DFS within 72 hours after it experiences certain categories of cyber incidents. In the proposed new rules, that category of incidents has been expanded to explicitly include ransomware. And here's another change that shows you how concerned the DFS is with ransomware and ransom payments. Under the proposed new rules, a covered entity would have to notify the DFS within 24 hours after making an extortion or ransom payment, after which the covered entity would have 30 days to explain why it made that payment, including an assessment of costs and benefits, and whether the company adequately informed itself about whether the payment would violate US and foreign sanctions rules.

[Kevin]: So we've highlighted five categories of changes in the new Part 500 cybersecurity rules: risk assessments, security controls, testing and training, new governance requirements, and new notice requirements. And believe it or not, there are other changes in these proposed new rules as well. The DFS is proposing the creation of a new class of companies called Class A companies. These are very large companies and they will be subject to additional requirements that non-class A companies are not subject to. The rules also speak to potential penalties and they incorporate the mitigating factors that are already in the banking law that may lead to reduced fines and penalties in the event that the department finds a covered entity liable.

[Kevin]: We'll talk about those in future episodes. So when will these proposed rule changes take effect? I mentioned earlier that we think it's likely to happen within the next 30 to 90 days. We're recording here today on February 4th. So basically we're looking at a window between March 1st and June 1st. Once the final rule takes effect, how long will you have to come into compliance? For most of the changes, it will be six months. For some of them, including the technical controls, you'll have more time. But at least one of the changes will take effect right away, and that is the requirement that a covered entity report a ransom payment within 24 hours. That change will take effect within 30 days.

[Kevin]: So what's the takeaway here? Should we be happy, sad, concerned, frustrated? Well, first and foremost, I think there's a lot of good here, particularly when it comes to MFA, passwords, vulnerability scans, pen testing, and even some of the governance requirements. Frankly, some of these things should probably have been implemented years ago. So it's a long time coming and we should be grateful. On the flip side, there are a lot of changes here, particularly technical ones, and I think it's going to take many covered entities, particularly the smaller ones, a great deal of time and resources to implement these changes. And it could, in many ways, be costly. So going forward, I think the best advice you're going to get from anyone is look at these proposed new changes now. Share them with your board and leadership and start thinking about the ways that you will be able to come into compliance when the final rule goes into effect.

[Kevin]: I hope you enjoyed this episode. If you have any questions or comments, please hit me up in the comments section below. I'd love to hear from you and please like, share, and subscribe. We really do appreciate your support. That's all for this episode. We're back soon with another one. Thanks.

[Kevin]: The *Cyber Sip* podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, Spotify, and Google Podcasts. Like, follow, share, and continue to listen.

Disclaimers:

This material is for informational purposes only and does not constitute legal advice or legal opinion. No attorney-client relationship has been established or implied. Thanks for listening.

Barclay Damon Live podcast transcripts and captions are automatically generated through artificial intelligence, and the texts may not have been thoroughly reviewed. The authoritative record of Barclay Damon Live programming is the audio file.